airmic

The EU General Data Protection Regulations

What risk managers need to know

BLM

Contents

BLM

BLM is the UK and Ireland's leading insurance and risk law specialist and our vision is to be recognised as one globally by 2020, building upon our already established international practice.

We are proud of our established and deep-rooted presence in the general insurance sector, the Lloyd's and London Market and amongst brokers. We also have a significant presence amongst corporate customers, the public sector and the health and care industry. The firm has an existing strong remit of international work and contacts, representing UK companies operating abroad, acting for a breadth of international organisations and handling high profile multijurisdictional cases.

Our team of over 200 partners and more than 800 legal specialists are dedicated to the insurance and risk market. Our purpose is to positively impact upon our customers' businesses and our sectors and our philosophy is delivering extraordinary outcomes for those customers, improving their business lives by reducing the time and money they spend on managing risk and resolving disputes. It's why they describe us as a firm with "its finger on the pulse of the market" and as a "technical powerhouse".

We're not afraid to challenge the status quo to help our customers achieve their objectives. Ultimately we do things The BLM Way for the benefit of our customers and colleagues.

For further information please visit **www.blmlaw.com**

1 Introduction

Data protection law originally came into being as a reaction to the misuse of personal data by totalitarian regimes before and during WW2.

It is intended to strike a balance between the rights of individuals to privacy and the capacity of businesses, organisations and governments to use personal data for their own purposes.

The computer and the internet have made it much easier and quicker to store, transfer and process personal data and have therefore exposed personal data to greatly increased risk of misuse, loss and theft. The EU and national governments have in response introduced a series of laws and regulations culminating in the General Data Protection Regulations ("GDPR") which will become law in the UK in June 2018 regardless of the Brexit vote.

The GDPR brings with it significant changes including mandatory breach reporting and very heavy fines. Information security is an organisation wide risk which necessitates physical and organisational as well as technical security measures.

Complying with both existing data protection law and the GDPR cannot therefore be sole responsibility of the IT team but must, rather, be treated as an issue for Risk Managers to address and control.

2 Current Law

In 1995 the Data Protection Directive was passed by the European Parliament. This was transposed into UK law by the Data Protection Act 1998 ('DPA'), which came into force on 1 March 2000 repealing the Data Protection Act 1984.

The DPA is based on 8 key principles which are enshrined within it:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of the data subject under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a territory or country outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The implementation of the DPA by businesses has been complicated by:

- The fact that the Data Protection Directive 1995 has been transposed into different and to some extent inconsistent national laws by individual countries within the EU
- The exponential growth in the use of the internet, smartphones, the paperless office and remote working coupled with rapid globalisation and the use of cloud computing services has changed the way in which individuals and businesses interact and the ways in which data is processed.
- The failure of data protection law to keep up with technological changes.
- The perceived cost and expense of effective cyber security and ignorance amongst individual industries and businesses within them about the cyber exposures that they face.

3 The GDPR

In order to address the risks posed to personal data and privacy by computers and the internet and to deal with the flaws in the existing data protection legislation the GDPR were launched in draft by the EU in 2012, discussed at length by representatives of member countries and approved by the European Parliament in 2016.

The GDPR will automatically become law without the need for national acts of parliament in all EU countries, including the UK, June 2018.

The GDPR clarifies and increases the responsibilities of organisations for the personal data that they handle and store and also introduces mandatory breach reporting and much tougher penalties for those who do not comply with data protection legislation.

Time will be needed to address the changes made by the GDPR and Risk Managers need to act now if they have not already started to do so.

3.1 The key changes are:

A requirement to notify breaches

Under the existing legislation in the UK there is no legal obligation to report data breaches to the Information Commissioner.
The new legislation includes a mandatory reporting requirement. Data controllers will have to notify personal data breaches to the competent supervisory authority (the Information Commissioner in the UK), where feasible, not later than 72 hours after becoming aware of the breach, unless the data controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of the data subjects concerned. Notifications must also be made to data subjects "without undue delay" if the breach is likely to result in a high risk to their rights and freedoms.

Much tougher fines

Under the current regime, Member States determine the fines, and/or criminal penalties, at local level. In the UK, at present, the Information Commissioner's Office only has the power to impose fines of up to £500,000 for serious breaches of the Data Protection Legislation. When the GDPR comes into force, however, the Information Commissioner's Office will be able to fine businesses up to €20 million or 4% of annual global turnover. For infringements not subject to administrative fines, Member States will have the power to set their own penalties, including criminal penalties.

The combination of mandatory reporting and much higher potential penalties under the GDPR is bound to raise awareness of data protection obligations and the need for businesses to comply with them.

Extra-territorial applicability

Businesses located outside the EU are currently not subject to EU data protection legislation. When the GDPR comes into force businesses located outside the EU will be subject to EU data protection legislation if they offer goods or services to individuals located within the EU, or if they monitor individuals' behavior which takes place within the EU.

This is likely result in many more international businesses becoming subject to the EU data protection law.

Application to both processors and controllers

The current data protection legislation imposes most of its obligations on data controllers only. Data processors are, therefore, currently far less regulated.

Article 3 of the GDPR provides that the new regulations will apply to the processing of personal data by both EU and non-EU controllers and processors.

The broader application to processors as well as controllers together with the fact that the GDPR will apply to businesses outside the EU that offer goods or services to individuals located within the EU, or monitor individuals' behavior which takes place within the EU will vastly increase the number of non-EU businesses which will need to be aware of and comply with the new regulations.

One Stop Shop – lead supervisory authorities

Under the current legislation data controllers that process data in more than one EU country can be subject at the same time to the different data protection laws of several EU countries. This creates complications.

One of the objectives of the new regulation is to create a "one stop shop" so that where processing activity affects data subjects in more than one Member State, the supervisory authority in the main establishment of the controller or processor (i.e. the country where most of the data processing takes place) will act as a "lead supervisory authority" and will regulate that particular activity across the EU.

Abolition of requirement to register as a data controller

The new regulations will abolish the requirement to register as a data controller.

Nevertheless, both data controllers and processors alike will be required to keep internal records of their data processing activities.

Data controllers may also be required to carry out a "data protection impact assessment" before processing personal data.

Processing children's data

It had been proposed that parental consent should be required in order to process personal data of children under 13. However, some EU countries rejected this proposal. Instead, it was agreed that each Member State can set their own limits for the age at which children no longer need parental consent at any age between 13 and 16. This could potentially significantly curtail the use of social media by young teenagers.

European Data Protection Board

A European Data Protection Board will be established to seek to ensure the consistent application of the GDPR across the EU. The Board will include representatives from each Member State, and its tasks will include issuing guidelines, recommendations, and opining on supervisory authorities' application of the GDPR.

The new Board will have a separate legal personality and will have the power to adopt binding decisions in disputes between Member State supervisory authorities.

A right to be forgotten

When a data subject no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.

Easier access to one's own data

Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way.

Right of data portability

It will be easier to transfer personal data between service providers.

4 Brexit

Notwithstanding the Brexit vote existing data protection law in the form of the DPA will remain in force subject to the changes made by the GDPR.

In our view Risk Managers must address the GDPR despite the Brexit vote because:

The ICO has recently confirmed that GDPR will come into force and become part of UK law before the UK leaves the EU.

Any business that has an EU presence or engages with EU companies will have to comply with the GDPR whether or not the UK is in the EU.

The changes effected by the GDPR are in general necessary and sensible.

5 How should you prepare for GDPR

Information security necessitates physical and organisational as well as technical security measures.

This in turn entails consciousness of the risks by board members, staff and management and the implementation and maintenance of rigorous staff policies and procedures expressed in concepts and language that they can understand.

In circumstances in which potentially crippling fines may be imposed for breaches, information security must be managed by an organisations risk manager and his/her team and cannot simply be left to the IT team to deal with.

In general terms, you should, in preparation for GDPR:

- Review your current data processing activities
- Perform impact assessments, to establish whether you have a risk of infringement of the GDPR;
- Establish necessary policies and processes to meet all GDPR requirements (E.G security, complaints handling, data accuracy, breach reporting, etc.).
- Update current policies regarding personal data and make the necessary changes to you business operations to ensure compliance with GDPR.

The ICO has helpfully identified 12 steps which should be taken now to prepare for GDPR:

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Consent

You should review how you are seeking, obtaining and recording consent.

Data breaches and data security

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

airmic

6 Lloyds Avenue
London
EC3N 3AX
Ph. +44 207 680 3088
Fax. +44 20 7702 3752
email: enquiries@airmic.com
www.airmic.com